Library Maintenance

A library is defined to Natural Security by creating a *library security profile*. The library security profile determines the conditions under which the library may be used. This section covers the following topics:

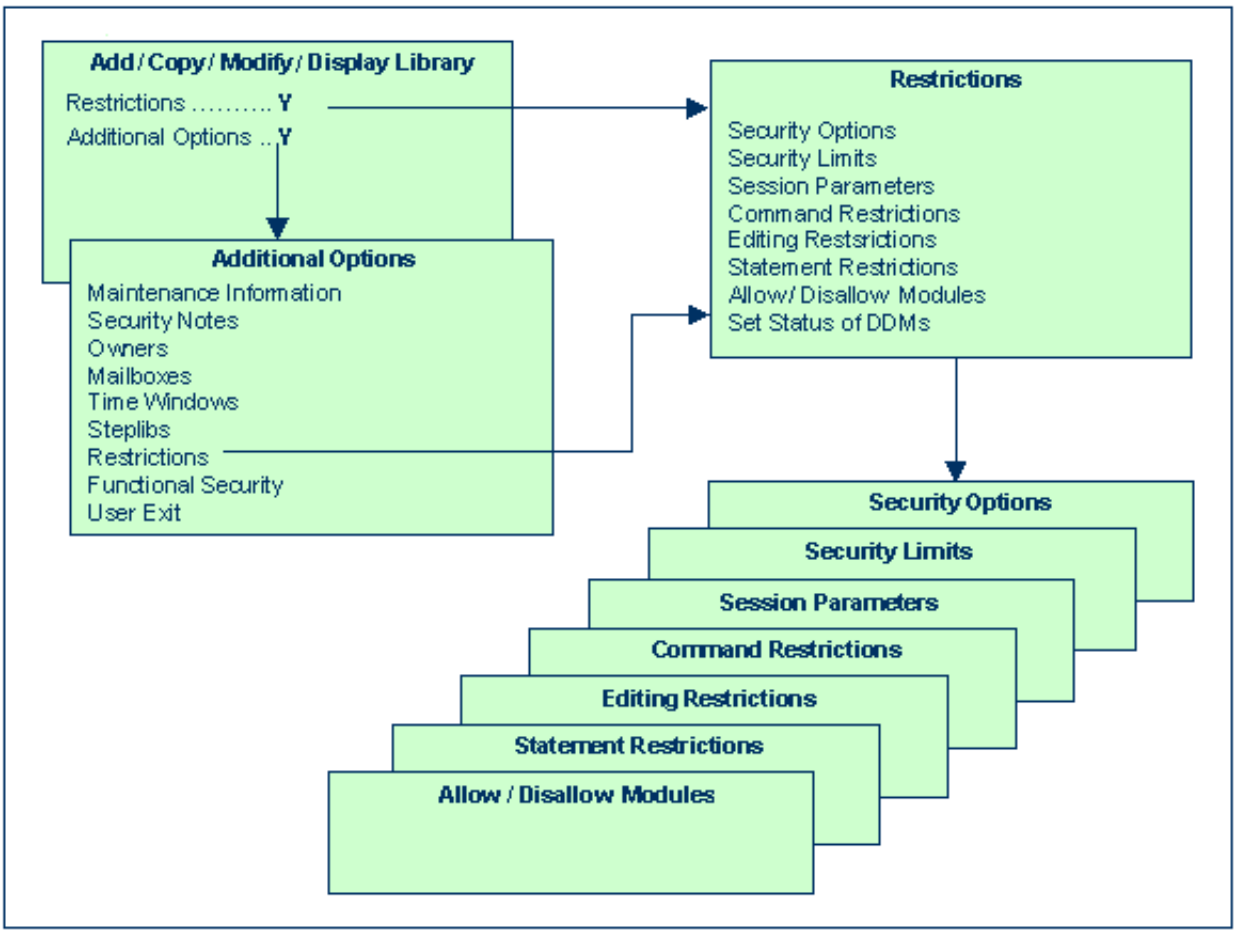
- Components of a Library Profile
- Creating and Maintaining Library Profiles

Components of a Library Profile

This section covers the following topics:

- Overview of Components
- Components on Main Library-Profile Screen
  - General Options
  - Library File
  - Transactions
- Additional Options
  - Restrictions:
    - Security Options
    - Security Limits
    - Session Parameters
    - Command Restrictions
    - Editing Restrictions
    - Statement Restrictions
    - Allow/Disallow modules
    - Set Status of DDMs

Overview of Components



Components on Main Library-Profile Screen

The following type of screen is the "basic" library security profile screen, which appears when you invoke one of the functions Add, Copy, Modify, Display for a library security profile:

```
14:00:00                  *** NATURAL SECURITY ***                  2003-04-13
                               - Modify Library -

                                              Modified .. 2002-06-20 by SAG
  Library ID ..... TESTLIB
  Library Name ... ____________________________

      General Options            Library File              Transactions
  -----------------------   -----------------------   ---------------------------
  People-protected .... Y   DBID ........ _____       Startup .......... ________
  Terminal-protected .. N   FNR ......... _____       Batch execution .. Y
  Restrictions ........ Y   Password .... ________    Restart .......... ________
  Logon recorded ...... Y   Ciphercode .. ________    Error ............ ________
  Utilities ........... O
  Programming mode .... R                             User exit ........ ________
  Cross-reference ..... N
  Restart ............. Y


  Additional Options ... N


  Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
        Help  PrevM Exit  AddOp Restr Flip                                 Canc
```

The individual items you may define as parts of a library security profile are explained below.

Field	Explanation
Library ID (display only)	The ID of the library as specified when the library security profile was created.
Library Name	You may enter a name for the library, which may be up to 32 characters long.

General Options

Field	Explanation
People-protected/ Terminal-protected	You may specify whether the library is to be *people-protected* and/or *terminal-protected* in order to restrict the use of the library. The possible combinations of protection are described under Protected Libraries in the section Protecting Libraries.
Restrictions	Special restrictions may be defined for the library, as described under Additional Options below. • If no restrictions are defined, the system profile defined in the Natural parameter module applies. • If restrictions are defined, the value of this field is automatically set to "Y". If you set it to "N" again, any specification you have made in the restrictions will automatically be deleted!
Logon recorded	This option determines whether logons to the library are to be recorded or not. **Y** Every time a user logs on to the library, a logon record will be written by Natural Security. You may review the activities of users by viewing these logon records (see Logon Records in the section Administrator Services for further information). **N** Logons to the library will not be recorded.

Utilities	For consistent control of Natural utility usage, **utility profiles** should be used; they are described in the section Protecting Utilities. The Natural utilities NATLOAD, NATUNLD, SYSERR, SYSMAIN, and SYSTRANS are used to process the contents of a library. This option determines who may process the contents of the library using a Natural utility for which no utility profiles are defined. This option only applies if the utility used is *not* controlled by utility profiles; otherwise it is ignored. Possible values for this option are: **N** **No protection** - The library's contents may be processed by any user. **O** **Permission for Owners** - The library's contents may be processed only by the *owners* of the library security profile. If no owner is specified, any user of type ADMINISTRATOR may do so. In the case of a private library, in addition to the owners, the user with the same ID as the library ID may also process the library's contents. In batch mode, please note that an owner who requires a countersignature from a co-owner cannot process the contents of the library (as countersignatures are not allowed in batch mode). **P** **Permission under Protection rules** - The library's contents may be processed under *protection rules*, that is, only by users who are allowed to log on to the library. For private libraries in private mode, the following applies: The user with the same ID as the library ID may process the library's contents; anyone else may process it only after entering that user's password (on a countersignature screen provided for that purpose). In batch mode, please note that a user cannot process the contents of another user's private library in private mode (as no password can be entered in batch mode). If the Natural system command SCAN is allowed for the library (see Command Restrictions below), the Utilities option also applies to the SCAN command.
Programming mode	Natural programming mode: **S** (= Structured mode) - The programming mode to be used cannot be changed with the Natural parameter SM, and structured mode will invariably be in effect. **R** (= Reporting mode) - The setting of the Natural profile/session parameter SM (described in the Natural Parameter Reference documentation) determines the mode to be used.
Cross-reference	This option determines whether an active cross-reference in Predict (if installed) will be generated for the library. **Y** Yes - An active cross-reference will be generated. **N** No - An active cross-reference will not be generated. **F** Force - An active cross-reference will be forced. **D** Doc - Objects to be cataloged must be documented in Predict. However, no active cross-reference will be generated. See the Predict documentation for details on active cross-references.

Restart	**Y** The library may be re-invoked by entering "RESTART" as the library ID on the logon screen; an Adabas OPEN command with End of Transaction ID (ETID) will be executed during the logon procedure. **N** The library cannot be "RESTARTed". The ETID specified in Natural Security will not be used for the Adabas OPEN command.
Version control (display only)	This field only applies on mainframe computers and if the library is under control of Predict Application Control. This field indicates the version control status of the library. If the library is controlled by Predict Application Control, the database ID (DBID) and file number (FNR) of the FDIC system file in which the library's Predict data are stored are also displayed.

Library File

The items under Library File concern the database file where the source programs and object modules contained in the library are to be stored.

Field	Explanation
DBID/FNR	The database ID and file number of the file. If no DBID/FNR are specified here, the DBID/FNR of the FUSER parameter as defined in the Natural parameter module/file apply (see the FUSER parameter in the Natural Parameter Reference documentation).
Password	This field only applies on mainframe computers, it has no effect under UNIX and Windows. If the library file is password-protected, the Adabas password (for VSAM files, the VSAM DDname) must be entered in this field to enable Natural to access the file.
Cipher code	This field only applies on mainframe computers, it has no effect under UNIX and Windows. If the library file is ciphered, the Adabas cipher code (for VSAM files, the VSAM password) must be entered in this field to enable Natural to access the file.
Read-only	If you wish the library file to be read-only, mark this field with an "X" (this corresponds to the RO option of the FUSER profile parameter).
ETID (display only)	This field contains the library-specific component of the ID for End of Transaction data (for details on ETIDs, see Components of a User Profile in the section User Maintenance).

Note:
For the Natural system libraries - that is, all libraries whose IDs begin with "SYS" (except the library SYSTEM) - you cannot enter a DBID, FNR, password, or cipher code. For these libraries the DBID, FNR, password, and cipher code of the Natural profile parameter FNAT (described in the Natural Parameter Reference documentation) as defined in the Natural parameter module/file invariably apply.

Transactions

Field	Explanation
Startup	You may enter the name of a startup transaction; this transaction will always be invoked immediately after a successful logon to the library. See also the Natural system variable *STARTUP. The name of the startup transaction will be placed in the Natural system variable *STARTUP. If it is also executed in batch mode, its name will be only be placed into *STARTUP if "Batch execution" (see below) is set to "S".
Batch execution	This field only applies if the Natural system variable *DEVICE is set to "BATCH" (otherwise its value has no effect). It determines whether the startup transaction specified in the library profile (see above) is also executed in batch mode. You can specify one of the following values: **Y** The startup transaction will also be executed (once) in batch mode. **S** The startup transaction will also be executed in batch mode; in addition, its name will be placed in the Natural system variable *STARTUP. **N** If the NEXT/MORE line is allowed for the library (see Security Options below), the startup transaction will *not* be executed in batch mode. If the NEXT/MORE line is *not* allowed, the startup transaction will also be executed (once) in batch mode. See also the section Natural Security In Batch Mode.
Restart	You may enter the name of a restart transaction; this transaction will always be invoked when the library is reinvoked by entering "RESTART" as the library ID on the logon screen.

Field	Explanation

Error	You may enter the name of an error transaction; this transaction will be invoked after the occurrence of an execution time error (if the program does not contain an ON ERROR statement, or if it does contain an ON ERROR block which is not exited with a FETCH, STOP, TERMINATE or RETRY statement); if the Natural profile parameter SYNERR is "ON", the error transaction may also handle syntax errors.
	
	The following parameters will be passed from the program in error to the error transaction:
	- error number (N4 if SG=OFF; N5 if SG=ON),
	- line number (N4),
	- status (A1),
	- program name (A8),
	- level (N2).
	The error transaction must be able to read these parameters.
	
	For example:
	
	`INPUT (SG=OFF) #ERROR (N4)`
	`#LINE (N4)`
	`#STATUS(A1)`
	`#PGM (A8)`
	`#LEVEL (N2)`
	
	The field #ERROR contains the error number.
	
	The field #LINE contains the number of the line in which the error occurred. (If the #STATUS is either "C" or "L", the line number will be "0".)
	
	The field #STATUS contains one of the following values:
	
	C = Command processing error.
	
	L = Logon error.
	
	R = error on Remote server (in conjunction with Natural RPC).
	
	O = Object time error.
	
	S = non-correctable Syntax error.
	
	The field #PGM contains the name of the program in which the error occurred.
	
	The field #LEVEL corresponds with the Natural system variable *LEVEL. The #LEVEL parameter is only passed on if the Natural profile parameter SYNERR is set to "ON".
	
	Note:
	If no error transaction is specified, the program specified with the Natural profile parameter ETA (described in the Natural Parameter Reference documentation) will receive control when an error occurs.
	If an error occurs during an initial logon, the program specified with the ETA parameter will also receive control (for other logon errors, the error transaction specified in the library*from which you log on* to another library applies).
	
	A sample error transaction program "ERROR" is provided in source form in the library SYSSEC.

User Exit

With each library profile and special link profile, you can store 250 bytes of additional data of your choice.

These additional data can be stored/read by means of a user exit subprogram which must contain a CALLNAT statement (with five parameters as described below) which in turn invokes one of the following subprograms:

- **SNAASEXT** - to store additional library data,
- **SNAAREXT** - to read additional library data,
- **SNAUSEXT** - to store additional special link data,
- **SNAUREXT** - to read additional special link data.

These four subprograms are contained in the Natural Security library SYSSEC.

In the User Exit field of the library profile or special link profile, you enter the name of the user exit that invokes one of the above subprograms.

To invoke the user exit, you mark "User Exit" with "Y" in the Additional Options window (see below).

If you wish to handle the additional data from within a library, you can also invoke the above subprograms by means of a user exit from a library itself. In this case you must copy the subprograms into that library (by using the SYSMAIN utility).
When invoked from a library, each subprogram will check and ensure that only data concerning that library or the specified link are read/stored.

In the security profiles of the Natural system libraries, that is, all libraries whose IDs begin with "SYS" (except the library SYSTEM), you cannot specify a user exit.

SNAASEXT is used to store additional library data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAASEXT	Contents returned from SNAASEXT
1st	A8	none	Library ID
2nd	A32	none	Library name
3rd	D	none	Date of latest modification
4th	A250	**Data to be stored**	same as passed
5th	B2	none	Return code

SNAAREXT is used to read addtional library data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAAREXT	Contents returned from SNAAREXT
1st	A8	none	Library ID
2nd	A32	none	Library name
3rd	D	none	Date of latest modification
4th	A250	none	**Data read**
5th	B2	none	Return code

When you invoke SNAAREXT or SNAASEXT from a library profile in SYSSEC, the data will refer to the library you are currently maintaining.

When you invoke SNAAREXT or SNAASEXT from outside SYSSEC, the data will refer to the library from which you invoke the subprogram.

SNAUSEXT is used to store additional special link data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAUSEXT	Contents returned from SNAUSEXT
1st	A8	none	Library ID
2nd	A8	User ID (must only be filled if SNAUSEXT is invoked from outside SYSSEC)	User ID
3rd	D	none	Date of latest modification
4th	A250	**Data to be stored**	same as passed
5th	B2	none	Return code

SNAUREXT is used to read additional special link data. It must be invoked with the following five parameters:

Parameter	**Format/Length**	**Contents passed to SNAUREXT**	**Contents returned from SNAUREXT**
1st	A8	none	Library ID
2nd	A8	User ID (must only be filled if SNAUREXT is invoked from outside SYSSEC)	User ID
3rd	D	none	Date of latest modification
4th	A250	none	**Data read**
5th	A2/B2	*****	Return code*****

***** When you invoke SNAUREXT from outside SYSSEC, you may read several special links to the library by using the 2nd parameter as start value and specifying one of the following operators in the 5th parameter (A2): "EQ", "=", "GT", "> ", "LT", "< ", "GE", ">=", "LE", "<=". These operators determine the read condition as compared against the 2nd parameter.
Return code (B2) "0" indicates that the specified special link has been found; any other value indicates that no such link has been found.

When you invoke SNAUREXT or SNAUSEXT from a special link profile in SYSSEC, the data will refer to the link you are currently maintaining.
When you invoke SNAUREXT or SNAUSEXT from outside SYSSEC, the data will refer to the link between the specified user ID and the library from which you invoke the subprogram.

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners
- Mailboxes
- Time Windows
- Steplibs
- Restrictions
- Functional Security
- User Exit

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window/screen will be displayed (in the order of the items in the selection window).

The Restrictions window can also be invoked directly by pressing PF5 on the basic security profile screen.

The individual options are explained below.

Additional Option	**Explanation**
Maintenance Information (display only)	In this window, the following information is displayed: • the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; • the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	In this window, you may enter up to eight IDs of ADMINISTRATORs. Only the ADMINISTRATORs specified here will be allowed to maintain this security profile. If no owner is specified, any user of type ADMINISTRATOR may maintain the library. For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID. For an explanation of owners and co-owners, see the section Countersignatures.
Mailboxes	In this window, you may enter up to five mailbox IDs. For information on mailboxes, see the section Mailboxes.
Time Windows	In this window, up to five time windows may be specified, outside of which the library cannot be used. For example, if a time window is set to "0815 - 1300", a user may log on to the library only between 08:15 h and 13:00 h; if a user is still logged on to the library at 13:00 h, the application contained in the library will automatically be terminated.

Additional Option	Explanation
Steplibs	In this window, you can enter the names of the libraries which are to be the steplib libraries (concatenated libraries) for the library. Multiple steplibs allow you to make different modules available to different libraries and also restrict the general availability of modules without having to have multiple copies of the same module in multiple libraries; that is, each module has to exist only once, but you can nonetheless make it available to several libraries, but not to others. For example, the modules that are to be available to all libraries can be contained in a general steplib which is specified in all library profiles, while modules that are to be available only to some libraries can be contained in another steplib which is specified only in some library profiles. Moreover, by specifying different special links to a library (see Linking Users to Libraries in the section Protecting Libraries), you can allow different users of the same library the use of different steplibs. You can specify up to 8 steplibs, plus a value for the Natural system variable *STEPLIB: When a programming object is requested in the library but not found in it, the 8 steplibs are searched - in the order in which they are specified in the library profile - for that object. If the requested object cannot be found in any of the 8 steplibs, the *STEPLIB library will be searched for it. If it cannot be found in that library either, the library SYSTEM will be searched for it (without SYSTEM having to be specified as a steplib in a library profile). If no value is specified in any of the 8 steplib fields in the library profile, the 8 steplibs specified with the Natural profile parameter LSTEP will be used instead. If no value is assigned to *STEPLIB in the library profile, the *STEPLIB value of the Natural profile parameter LSTEP will be used instead. **Notes:** Owner logic applies to the specification of a steplib; that is, if owners are specified in a library profile (see above), only these owners will be allowed to enter the library as steplib in the profile of another library. For Natural system libraries (that is, libraries whose IDs begin with "SYS") - except library SYSTEM - you cannot specify a *STEPLIB library. For these libraries, an internal system steplib is used as *STEPLIB library. If you use the library SYSTEM as steplib only, SYSTEM itself need not be defined as a library to Natural Security. Next to each steplib name, you can enter a database ID (DBID), file number (FNR), password and cipher code in the steplib window of a library window. If you assign "99999" as DBID value for a steplib in the steplib window of a library profile, the DBID value specified in the library profile of the steplib will be used. The same applies to FNR, password and cipher code values. If you assign no DBID value (or "0") for a steplib in the steplib window of a library profile, the DBID value of that library will be used. The same applies to FNR, password and cipher code values. By marking a steplib name with the cursor and pressing PF5 in the steplib window of a library profile, you can copy the actual values of DBID, FNR, password and cipher code from the steplib profile into the steplib window. For the *STEPLIB library specified in a library profile, the DBID, FNR, password and cipher code values of that library profile apply.

Additional Option	Explanation
Restrictions	As part of the restrictions, you may define: • Security Options • Security Limits • Session Parameters • Command Restrictions • Editing Restrictions • Statement Restrictions • Allow/Disallow modules • Set Status of DDMs These items are described below.
Functional security	In this window, you may define functional security for the command processors of the library.This is only relevant if command processors have been created with the Natural utility SYSNCP. See the section Functional Security for details.
User exit	If a user exit is specified in the Transactions column of the main library security profile screen, you can activate that user exit by marking this field.

Security Options

If you mark "Security Options" in the Restrictions selection window with any character, the Security Options window will be displayed. In this window, you can set the following options:

Option	Explanation
Allow NEXT/MORE line	**Y** - Allows the use of the Natural main menu. **N** - Suppresses the Natural main menu; when a user logs on to the library, the startup transaction specified for the library will be invoked instead (if no startup transaction is specified, the logon procedure will be invoked; see also the Natural system variable *STARTUP).
Allow system commands	**Y** - Allows the use of Natural system commands in the library. To disallow individual commands, you use the Command Restrictions section of the library profile (see below). **N** - Disallows the use of all system commands in the library. (This does not affect the system commands FIN, LAST, LASTMSG, LOGOFF, LOGON, MAINMENU, RENUMBER, RETURN, SETUP and TECH; they can always be used.)
Execution of update programs	**Y** - Programs that update the database can be executed in the library. **N** - Programs that update the database cannot be executed in the library.
Device	If this field is left blank, use of the library will not be restricted to any operation mode or device. If you enter a value, use of the library will be restricted to one specific device or operation mode. Possible values are: ASYNCH, BATCH, BTX, COLOR, PC, TTY, VIDEO and WS-CON (according to the current values of the Natural system variable *DEVICE).
Clear source area by logon	**N** - The editor source work area will *not* be cleared when a user logs on from the library to another. **Y** -The work area of the editor will be cleared automatically when a user logs on from the library to another.
PC download/ PC upload	**Y** - Modules contained in the library can be downloaded from the mainframe to a personal computer and uploaded from a personal computer to the mainframe respectively. **N** - Download and upload of modules will not be possible. This field only applies to mainframe computers; it has no effect under UNIX and Windows.
Close databases by logon	**Y** -All databases that have been accessed during the current Natural session will be closed automatically when a user logs on from the library to another. **N** - No databases will be closed when a user logs on from the library to another.

Security Limits

If you mark "Security Limits" in the Restrictions selection window with any character, the Security Limits window will be displayed. In this window, you can set the following limits:

Limit	Explanation
Non-activity logoff limit	The maximum time (in seconds) which may elapse after the last terminal communication. If this time is exceeded, a new logon procedure will be invoked as soon as the next input is received from the terminal. Possible values are 0 - 99999. If you wish no limit to be in effect, set this field to "0".
Maximum transaction duration	The maximum time (in seconds) permitted for a single Adabas transaction. This feature can be used to prevent the blockage of resources for an excessive time. If the time is exceeded, the current transaction will be backed out. Possible values are 0 - 99999. If you wish no limit to be in effect, set this field to "0". The Natural system variable *TIME-OUT contains the time remaining before a time-out will occur. (The Adabas TT parameter (Adabas transaction time limit) will be checked separately).
Maximum number of source lines	The maximum number of source-code lines permitted for a user-written Natural program. If the line limit is exceeded, the Natural syntax checker will issue an appropriate error message. Possible values are 0 - 9999.
Maximum amount of CPU time (MT)	The maximum amount of CPU time (in seconds) to be used (as in the Natural profile parameter MT, described in the Natural Parameter Reference documentation). If you set this field to "0", the limit is determined by the value of the Natural profile parameter MT. If you wish the highest possible limit to be in effect, set this field to the maximum value (9999999). If you wish no limit to be in effect, set this field to "9999999999". This field only applies to mainframe computers; it has no effect under UNIX and Windows.
Maximum number of Adabas calls (MADIO)	The maximum number of Adabas calls permitted between two screen I/O operations (as in the Natural profile parameter MADIO, described in the Natural Parameter Reference documentation). If the number specified is exceeded, the Natural program will be interrupted and an appropriate error message displayed. If you set this field to "0", the limit is determined by the value of the Natural profile parameter MADIO. If you wish the highest possible limit to be in effect, set this field to the maximum value (32767). If you wish no limit to be in effect, set this field to "99999".

Maximum number of program calls (MAXCL)	The maximum number of program calls permitted between two screen I/O operations (as in the Natural profile parameter MAXCL, described in the Natural Parameter Reference documentation). If the number specified is exceeded, the Natural program will be interrupted and an appropriate error message displayed. If you set this field to "0", the limit is determined by the value of the Natural profile parameter MAXCL. If you wish the highest possible limit to be in effect, set this field to the maximum value (32767). If you wish no limit to be in effect, set this field to "99999".
Processing loop limit (LT)	The maximum number of records which may be read in any given processing loop of the library (as in the Natural profile parameter LT, described in the Natural Parameter Reference documentation). If you set this field to "0", the limit is determined by the value of the Natural profile parameter LT. If you wish the highest possible limit to be in effect, set this field to the maximum value (2147483647). If you wish no limit to be in effect, set this field to "9999999999".

Session Parameters

If you mark "Session Parameters" in the Restrictions selection window with any character, the Session Parameters screen will be displayed.

On this screen, you may specify values for Natural session parameters, which will override the default parameter values set during Natural installation.

The parameters in the top left-hand block of the screen may take the following values. If a parameter is left blank, the corresponding default character will be valid.

Parameter	Possible Values
DC	Any character.
CF	Any special character, or "F" (for OFF).
CLEAR	Any character.
IA	Any special character.
IM	"F" (Forms mode) or "D" (Delimiter mode).
ID	Any special character.

The parameters in the top right-hand block of the screen may take the following values. If a parameter is left blank, the corresponding default value will be valid.

Parameter	Possible Values
SA	"T" (true) or "F" (false).
DU	For mainframe computers: "O" (on), "N" (off) or "F" (force). For all other platforms: "O" (on) or "N" (off).
EJ	"T" (true) or "F" (false).
FS	"T" (true) or "F" (false).
WH	"T" (true) or "F" (false).
ZD	"T" (true) or "F" (false).

The parameters in the bottom right-hand block of the screen may take numeric values. If a parameter is left blank or specified as "0", the corresponding default value will be valid.

Parameter	Possible Values
LS	Numeric value.
PS	Numeric value.
SL	Numeric value.
SF	Numeric value.

For information on the individual session/profile parameters, see the Natural Parameter Reference documentation.

Moreover the screen provides the following fields:

Field	Explanation
Adabas open (OPRB)	The contents of the record buffer used with the Adabas OPEN command may be entered. If so, a restricted OPEN will be executed, which means that only files included in the record buffer may be referenced. If no record buffer contents are specified, all accessible files may be referenced (see also the Adabas Command Reference documentation). If this field is set to "NOOPEN", no Adabas OPEN command will be executed. If this field is left blank, an OPRB parameter specified dynamically when invoking Natural applies for this library (see the Natural Parameter Reference documentation for details on the profile parameter OPRB).
Spool profile	The name of the spool profile may be entered (only applicable if Natural Advanced Facilities is installed; see the Natural Advanced Facilities documentation for details).
Adabas password	The Adabas password used for access to the Adabas data files (not system files) referenced by the library. This is only relevant if the corresponding files are password-protected under Adabas Security. The password specified in the security profile applies to all database access statements for which neither an individual password is specified nor a PASSW statement applies. It applies within the library in whose security profile it is specified, and also remains in effect in other libraries you subsequently log on to and in whose security profiles no password is specified. See also the PASSW statement in the Natural Statements documentation.

Natural RPC Restrictions

When you press PF8 on the Session Parameters screen, another screen will be displayed in which you can set various restrictions that apply when subprograms contained in the library are executed by means of Natural RPC in a client/server environment.

These restrictions are only relevant for library security profiles defined on the client.

Field	Explanation
Expiration Criteria	The following criteria determine how often / how long subprograms in the library can be executed by means of Natural RPC. When one of the criteria is reached, the criteria can either be reset by means of the user exit USR1071 or by the user newly logging on to the library.
Use Count	Determines how many times remote subprograms can be executed. A value of "0" means that no such limit is in effect.
Number of Days	Determines for how many days remote subprograms can be executed. The days are counted beginning with the logon to the library. A value of "0" means that no such limit is in effect.
Number of Hours/Minutes	Determines for how many hours/minutes remote subprograms can be executed. The time is counted beginning with the logon to the library. A value of "0" means that no such limit is in effect.
Allow Overwriting by User Exit USR1071	**Y** - The above expiration criteria in the library security profile, as well as the user ID and password from the client logon procedure, can be overwritten by criteria specified with user exit USR1071. **N** - No data can be set/overwritten by user exit USR1071.
Close All Databases	This option allows you to control the logon-/logoff-dependent closing of databases. It affects all databases which have been opened by remote subprograms contained in the library: **N** - The databases are *not* closed when a logon/logoff to/from the library is performed. **Y** -The databases are closed when a *logon* to the library is performed. **F** - The databases are closed when a *logon* to the library is performed, and when a *logoff* from the library is performed. This option is only relevant if the option LOGONRQ=ON is set in the Natural profile parameter RPC or NTRPC macro. If you wish to have one user-queue element per client session for each database accessed by the RPC server, it is recommended that you set LOGONRQ=ON and "Close All Databases" to "Y" or "F".

Logon Option	This option determines which logon data are evaluated when the library is accessed by the RPC server: **N** - Library ID, user ID and password are evaluated. **E**- Library ID, user ID and password are evaluated; in addition, it is checked if the user ID used for the access to the RPC server (for example, via the user exit USR1071) is identical to the user ID supplied via the user exit USR2071. **A** - Only library ID and user ID are evaluated (similar to the Natural profile parameter AUTO=ON, but for this library only). **S** - Only library ID and user ID are evaluated (similar to the Natural profile parameter AUTO=ON, but for this library only); in addition, it is checked if the user ID used for the access to the RPC server (for example, via the user exit USR1071) is identical to the user ID supplied via the user exit USR2071.

User exits USR1071 and USR2071 are contained in library SYSEXT. For further information on Natural RPC with Natural Security, see the sections Using Natural RPC With Natural Security and Logon To A Server Library in the Natural Remote Procedure Call documentation.

Command Restrictions

If you mark "Command Restrictions" in the Restrictions selection window with any character, the Command Restrictions screen will be displayed. On this screen, you may allow or disallow the use of individual Natural system commands.

By default, all commands shown on the Command Restrictions screen are marked with "Y", which means that all commands are allowed.

- Mark with "Y" each command you wish to be available for use in the library.
- Mark with "N" each command you wish *not* to be used in the library.

For information on the individual commands, see your Natural System Command Reference documentation.

Those commands which are displayed intensified on the Command Restrictions screen use the Natural syntax checker and consequently Natural statements (which may also be allowed/disallowed individually; see Statement Restrictions below).

Restricting the Use of the SCAN Command

You can either disallow the system command SCAN altogether for a library via the Command Restrictions (as described above), or you can control its use via the Utilities option:

- If SCAN is marked with "N" on the Command Restrictions screen, the SCAN command cannot be used in the library (regardless of the Utilities option).
- If SCAN is marked with "Y" on the Command Restrictions screen, the Utilities option (in the General Options part of the library profile) determines who may use the SCAN command in the library. The Utilities option may take one of the following values:

N	**No protection** - The SCAN command may be used in the library by any user.
O	**Permission for Owners** - Only the owners of the library may use the SCAN command; if no owner is specified, any user of type ADMINISTRATOR may use it. In a private library in private mode, in addition to the owners, the user with the same ID as the library ID may use the SCAN command. In batch mode, please note that an owner who requires a countersignature from a co-owner cannot use the SCAN command (as countersignatures are not allowed in batch mode).
P	**Permission under Protection rules** - The People/Terminal protection of the library applies: Only users who may use the library - and only under the conditions under which they may use it - may use the SCAN command. For a private library in private mode, the following applies: The user with the same ID as the library ID may use the SCAN command; anyone else may use it only after entering that user's password (on a countersignature screen provided for that purpose). In batch mode, please note that a user cannot use the SCAN command in another user's private library in private mode (as no password can be entered in batch mode).

Editing Restrictions

If you mark "Editing Restrictions" in the Restrictions selection window with any character, the Editing Restrictions window will be displayed. In this window, you may allow or disallow the editing of Natural objects of certain object types.

By default, all object types shown in the Editing Restrictions window are marked with "Y", which means that objects of all types may be edited.

- Mark with "Y" each type of object whose editing you wish to be allowed in the library.
- Mark with "N" each type of object whose editing you wish *not* to be allowed in the library.

For information on Natural object types, see the Natural Programming Guide; for information on the Natural editors, see your Natural Editors documentation.

To disallow editing altogether, you may disallow the use of the EDIT command (see Command Restrictions above). When you disallow the EDIT command, all object types in the Editing Restrictions window are automatically marked with "N". When you allow the EDIT command again, all object types in the Editing Restrictions window are automatically marked with "Y" again.

Statement Restrictions

If you mark "Statement Restrictions" in the Restrictions selection window with any character, the Statement Restrictions screen will be displayed. On this and the next screen, you may allow or disallow the use of individual Natural statements. To get from this screen to the next and back again, you press PF7 and PF8 respectively.

By default, all statements shown on the Statement Restrictions screen are marked with "Y", which means that all statements are allowed.

- Mark with "Y" the Natural statements you wish to be allowed for use in the library.
- Mark with "N" the Natural statements you do *not* wish to be used in the library.

For the FIND statement and other database access statements, you may also allow/disallow individual clauses.

Any Natural statement which is not listed on the Statements Restrictions screen is always allowed (for example, the statement END).

Disallow/Allow Modules

In the Restrictions selection window, besides the field you mark to select "Disallow/Allow Modules", there is a second field, in which you can enter one of the following:

X	This causes all modules to be allowed; individual modules cannot be disallowed (the Disallow/Allow Modules screen will not be invoked). If you enter an "X", do not at the same time mark the selection field.
D	All modules are initially allowed, and you may disallow individual modules.
A	All modules are initially disallowed, and you may allow individual modules.

Note:
For the Display function, you can only mark the selection field; regardless of the setting of the second field, the Disallow/Allow Modules screen will be displayed showing the list of allowed/disallowed modules.

If you mark "Disallow/Allow Modules" in the Restrictions selection window with any character and enter a "D" or "A" in the second field, the Disallow Modules screen or Allow Modules screen respectively will be displayed:

```
11:13:46                    *** Natural Security ***                2003-04-13
                               - Disallow Modules -
   Library  TESTLIB                          0 Module names not held in user buffer
   Module   T Status                  Mark  Module   T Status                 Mark
   ------------------------------------  ------------------------------------
   #ABANDON P ALLOWED                   _  #UAFLAG1 P ALLOWED                  _
   #ATRAIL  P ALLOWED                   _  #UAFLAG2 P ALLOWED                  _
   #BOC     P ALLOWED                   _  #UAFLX   P ALLOWED                  _
   #DAWG    P ALLOWED                   _  #UB      P ALLOWED                  _
   #KEY1    P ALLOWED                   _  #UBFLAG  P ALLOWED                  _
   #KEY2    P ALLOWED                   _  #UBFLAGB P ALLOWED                  _
   #MEDUSA  P ALLOWED                   _  AMAIL    P ALLOWED                  _
   #NEMESIS P ALLOWED                   _  APROFILE P ALLOWED                  _
   #PWINDOW P ALLOWED                   _  CALDANDO N ALLOWED                  _
   #TFECHO1 P ALLOWED                   _  HOTTA    M ALLOWED                  _
  *********************  Module Names held in User Buffer  **********************
    _________          _________          _________          _________          _________
    _________          _________          _________          _________          _________
  ------------------------------------------------------------------------------
  Reposition to .. _________    Display module names not held in UB .. _


  Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
        Help  PrevM Exit  AddOp Restr Flip  -     +     Free  Stepl       Canc
```

Column "T" on the Disallow/Allow Modules screen indicates the object types of the modules:

P	Program
N	Subprogram
S	Subroutine
H	Helproutine
G	Global data area
L	Local data area
A	Parameter data area
M	Map
C	Copycode
3	Dialog
4	Class

On the Disallow/Allow Modules screen, mark with a "D" the modules contained in the library you wish to be disallowed; mark with an "A" the modules contained in the library you wish to be allowed. The first ten module names marked will be held in the user buffer.

In addition, the following subfunctions are available:

Module Names Held in User Buffer	If you wish modules to be disallowed/allowed and their names to be held in the user buffer, type in their names into the ten fields provided on the Disallow/Allow Modules screen. If you type in a value followed by an asterisk (*), all module names beginning with that value will be disallowed/allowed and held in the user buffer. Those disallowed/allowed module names not held in the user buffer may be displayed by marking the "Display module names not held in User Buffer" field with any character. Unmark it to return to the Disallow/Allow Modules screen. If possible, the number of allowed/disallowed modules should not exceed 10; that is, all allowed/disallowed module names should be held in the user buffer; module names not held in the user buffer will cause a reduction in performance, as the Natural Security data file will have to be additionally accessed to check whether a module whose name is not held in the user buffer is allowed or not.
Allowing/Disallowing "Non-Existent" Modules (PF9)	The Disallow/Allow Modules screen of a library profile displays a list of all modules contained in the corresponding library. However, there may be modules which currently are not physically available (for example, because the corresponding database is not active, or the modules have not yet been written), and which would therefore not appear in the list of modules. Or in a heterogeneous production environment using a central mainframe FUSER system file, the library may exist not on the mainframe FUSER system file but in the file system on another platform. If you were to define a library profile for such a library, Natural Security on the mainframe computer would not know of that library, and the list of modules would therefore be empty. To enable you to disallow/allow such "non-existent" modules, the Allow/Disallow Modules function provides the subfunction "Free List of Modules". With this subfunction, you can predefine modules which are not physically present on the current FUSER system file. To invoke the subfunction, you press PF9 on the Disallow/Allow Modules screen. The "Free List of Modules" window will be displayed. In this window, you manually enter the names of modules and allow/disallow them.
Steplibs (PF10)	This function does not apply on mainframe computers. With this subfunction, you can disallow/allow modules in the library’s steplibs. To invoke the subfunction, you press PF10 on the Disallow/Allow Modules screen. A list of all the library’s steplibs will be displayed. On the list, you select the library whose modules you wish to disallow/allow. Then, the list of modules contained in the selected steplib will be displayed, which you can then disallow/allow individually. When you disallow/allow modules in a steplib in this way, this does not mean you actually disallow/allow these modules in the library profile of the steplib. The steplib modules are only disallowed/allowed with respect to usage by the library whose profile you are currently maintaining (that is, the library from within whose library profile you have invoked the subfunction).

Set Status of DDMs

This option only applies if the general option "Transition Period Logon" (see the section Administrator Services) is set to "N". It only affects DDMs for which no security profiles have been defined.

With this option, you can set the status of all new DDMs to PUBLIC. On mainframes, this applies to the file status; on UNIX and Windows, this applies to both the internal and the external status of DDMs.

In the Restrictions window, you can specify one of the following values for this option:

UNDF	The status of all DDMs without security profiles is undefined.
PUBL	The status of all DDMs without security profiles is PUBLIC.

By default, this option is set to "UNDF", which means that DDMs for which no security profiles have been defined cannot be used.

If you set this option to "PUBL", the status of all DDMs for which no security profiles have been defined is assumed to be PUBLIC, which means that these DDMs can be used. This allows you to use these DDMs without having to define security profiles for them.

For further information, see the sections Protecting DDMs On Mainframes and Protecting DDMs On UNIX and Windows.

Creating and Maintaining Library Profiles

This section describes the functions used to create and maintain library profiles. It covers the following topics:

- Invoking Library Maintenance
- Adding a New Library
- Selecting Existing Libraries for Processing
- Copying a Library
- Modifying a Library
- Renaming a Library
- Deleting a Library
- Displaying a Library
- Creating and Maintaining a Private Library

Invoking Library Maintenance

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark object type "Library" with a character or with the cursor. The Library Maintenance selection list will be displayed.

From this selection list, you invoke all library maintenance functions as described below.

Adding a New Library

The Add Library function is used to define new libraries to Natural Security, that is, create library security profiles.

Note:
To create library security profiles for *system libraries* (that is, libraries whose names begin with "SYS") more easily, you can use the Administrator Services function "System-library definitions", which provides predefined security profiles for most system libraries.

To add a new library security profile, enter the command ADD in the command line of the Library Maintenance selection list.

A window will appear. In this window, you enter a *library ID* (and, optionally, the ID of a *default profile*).

The Add Library screen will be displayed. On this screen, you may define a security profile for the library.

The Add Library screen and the subsequent screens/windows that may be part of a library security profile as well as the individual items you may define are described under Components of a Library Profile above.

When you add a new library, the owners specified in your own user security profile will automatically be copied into the library security profile you are creating.

Library ID

Library IDs are used by Natural Security to identify libraries and their security profiles.

A library ID may be 1 to 8 characters long, it must start with an upper-case alphabetical character, and it must be unique. A library ID must not contain blanks. It may consist of the following characters: upper-case alphabetical characters, numeric characters, hyphen (-) and underscore (_).

Before you start defining libraries, it may be advisable to conceive a logical system of creating library IDs that are related to the library names, as this will help you to identify libraries more easily when maintaining Natural Security.

Default Profile

When you add a new library, you can either type in every item within the library security profile by hand; or you can use a pre-defined default library profile as the basis for the security profile you are creating.

Before you use default library profiles, you should be familiar with the "normal" way of defining libraries (that is, without default profile).

Default profiles are created and maintained in the Administrator Services subsystem.

If you specify the ID of a default profile in the Add Library window, the items from the default profile will be copied into the library profile

On the Add Library screen, you can overwrite the items copied from the default profile, and specify further items.

For further information on default library profiles, see Library Default Profiles in the section Administrator Services.

Selecting Existing Libraries for Processing

When you invoke Library Maintenance, a list of all libraries that have been defined to Natural Security will be displayed.

If you do not wish to get a list of all existing libraries but would like only certain libraries to be listed, you may use the Start Value and Type/Status options as described in the section Finding Your Way In Natural Security.

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed. In the window, mark object type "Library" with a character or with the cursor (and, if desired, type in a start value and/or protection status). The Library Maintenance selection list will be displayed:

```
12:47:45                  *** NATURAL SECURITY ***                 2003-04-13
                            - Library Maintenance -

 Co Library ID Library Name                        Prot. Message
 __ __________ _____________________________      _____ ________________________
 __ KETEST                                        YN
 __ KEX        TEST APPL-KE                       YN
 __ KE1        KETEST                             NN
 __ KJH                                           NN
 __ KK-APPL                                       NN
 __ KKAPP                                         NN
 __ KKAPPC                                        NN
 __ KKAPP1                                        NN
 __ KKAPP2                                        NN
 __ KKAPP3                                        NN
 __ KKAPP4                                        YN
 __ KKAPP7                                        NN
 __ KKITEST                                       NN
 __ KKPAC                                         NN
 __ KKPROD                                        NN

 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit              Flip  -     +                       Canc
```

For each library, the ID, name and protection status are displayed.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

The following library maintenance functions are available (possible code abbreviations are underlined):

Code	Function
CO	Copy library
MO	Modify library
RE	Rename library
DE	Delete library
DI	Display library
LU	Link users to library
LF	Link library to files (this function is only available on mainframe computers)
MD	Modify DDM restrictions in library (this function is only available on UNIX and Windows)
EP	Protect environments

To invoke a function for a library, mark the library with the appropriate function code in column "Co".

You may select various libraries for various functions at the same time; that is, you can mark several libraries on the screen with a function code. For each library marked, the appropriate processing screen will be displayed. You may then perform for one library after another the selected functions.

Copying a Library

The Copy Library function is used to define a new library to Natural Security by creating a security profile which is identical to an existing library security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - *except* the owners (these will be copied from your own user security profile into the new library security profile you are creating).

In addition to duplicating a library profile, you can choose to also copy its links and utility profiles, as well as the actual library itself; this depends on the options described below.

How to Copy

On the Library Maintenance selection list, mark the library whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, specify the following:

To library	Enter the ID of the "new" library.
With links	Enter "Y" or "N". With this option, you can, in addition to the library profile, also copy its links and utility profiles; see below for details.
With Natural objects	Enter "Y" or "N". With this option, you can duplicate the actual library itself. This means that a new library will be created on the FUSER system file, and all Natural programming objects contained in the existing library will be copied into this new library. (Internally this option uses the MAINUSER application interface of the Natural utility SYSMAIN.)

The Copy Library screen will be displayed, showing the new library security profile.

The individual components of the security profile you may define or modify are described under Components of a Library Profile above.

With Links

If you leave the "N" in the "with links" field of the Copy Library window:

- any links defined for the existing library will not apply to the new library;
- any library-specific and user-library-specific utility profiles for the existing library will not apply to the new library.

If you enter a "Y" in the "with links" field of the Copy Library window,

- any links that exist for the existing library are copied for the new library, and you have the option to cancel the links you wish not to apply to the new library;
- any library-specific and user-library specific utility profiles that exist for the existing library are copied for the new library.

The procedure is as follows:

- Once you have made any changes to the copied security profile and then leave the Copy Library screen by pressing PF3, a list of users is displayed: the list contains all users which are linked to the existing library.
- On the list, you may mark individual users with "CL" to cancel any links you wish *not* to apply to the new library; all users you do not mark will automatically be linked to the new library in the same manner - normal or special link - as the existing library.

- Once you have established all user links and leave the list of users by pressing PF3, a list of files is displayed: the list contains all files/DDMs to which the existing library is linked.
- On the list, you may mark individual files/DDMs with "CL" to cancel any links you wish *not* to apply to the new library; to all files/DDMs you do not mark the new library will automatically be linked in the same manner - read or update link - as the existing library.

Modifying a Library

The Modify Library function is used to change an existing library security profile.

On the Library Maintenance selection list, you mark the library whose security profile you wish to change with function code "MO". The security profile of the selected library will be displayed.

The individual components of the security profile you may define or modify are described under Components of a Library Profile above.

Renaming a Library

The Rename Library function allows you to change the library ID of an existing library security profile.

On the Library Maintenance selection list, you mark the library whose ID you wish to change with function code "RE".

A window will be displayed in which you can enter a new ID for the library (and, optionally, change its name).

Depending on the setting of the general option "Deletion of non-empty libraries allowed" (as explained in the section "Administrator Services"), it may not be possible to rename a library security profile if the library contains any sources or object modules.

With Natural Objects

When you rename a library profile, this option allows you to also change the name of the actual library. This means that the library will be renamed on the FUSER system file, and all Natural programming objects contained in the library will be stored under the new library name. (Internally this option uses the MAINUSER application interface of the Natural utility SYSMAIN.)

Deleting a Library

The Delete Library function is used to delete an existing library security profile.

On the Library Maintenance selection list, you mark the library you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete Library function and should then decide against deleting the given library security profile, you may leave the Delete Library window by pressing ENTER without having typed in anything.
- If you wish to delete the given library security profile, enter the library’s ID in the window to confirm the deletion.

When you delete a library, all existing links to the library will also be deleted.

Depending on the setting of the general option "Deletion of Non-empty Libraries Allowed" (described in the section Administrator Services), it may not be possible to delete a library security profile if the library still contains any sources or object modules.

If you mark more than one library with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each library security profile by entering the library's ID, or whether all libraries selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a library accidentally.

With Natural Objects

When you delete a library profile, this option allows you to also delete the actual library itself. This means that the library - and all Natural programming objects it contains - will be deleted from the FUSER system file. (Internally this option uses the MAINUSER application interface of the Natural utility SYSMAIN.)

Displaying a Library

The Display Library function is used to display an existing library security profile.

On the Library Maintenance selection list, you mark the library whose security profile you wish to view with function code "DI". The security profile of the selected library will be displayed.

The individual components of the security profile are described under Components of a Library Profile above.

Creating and Maintaining a Private Library

Defining a Private Library

To define a private library to Natural Security, first mark the "Private Library" field in the user's security profile with "Y" (on the Add User, Copy User or Modify User screen) (marking this field does not cause any default private library profile to be created).

In the Additional Options window, you then select "Private Library"; or you press PF5 on the main user profile screen.

A Private Library screen will be displayed; the screen is identical to a "normal" library security profile screen (except when private libraries are used in private mode, in which case the screen does not contain the fields "People-protected" and "Terminal-protected"). On this screen and the subsequent screens/windows you define the security profile for the private library.

The library ID by which a private library is defined to Natural Security is identical to the respective user ID.

Maintaining a Private Library

In private mode, maintenance of existing private library profiles is performed via User Maintenance.

In public mode, private libraries also appear on the Library Maintenance selection list along with the other libraries, that is, they can be maintained like "normal" libraries with the library maintenance functions described above.

Deleting a Private Library

If private libraries are used in public mode, you delete a private library like any other library (see Deleting a Library above).

If private libraries are used in private mode, you delete a private library by marking the "Private Library" field in the user's security profile with "N". A window will be invoked in which you confirm the deletion by typing in the library ID.

Depending on the setting of the general option "Deletion of Non-empty Libraries Allowed" (described in the section Administrator Services), it may not be possible to delete a private library if it still contains any source or object modules.

